IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

IN RE: CDK GLOBAL DATA SECURITY BREACH LITIGATION This Document Relates to: All Cases	Case No. 1:24-cv-05221 **JURY TRIAL DEMANDED**

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

Consumer Plaintiffs Carol Berman, Thomas Kallas, and Eugene Baraga and Employee/Consumer Plaintiffs Michael Carvelli, Victoria Coombs, Christopher Gordish, and Dustin Leeberg, (collectively, "Plaintiffs"), individually and on behalf of the class(es) of similarly situated persons defined below, allege the following against Defendant CDK Global, LLC, ("Defendant" or "CDK"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. "A dealership in Phoenix [was] handwriting paper contracts and gauging creditworthiness with guesswork. A Jeep owner in Alabama [kept] calling about when a replacement part w[ould] be in stock. A family in New Jersey [was] waiting for word on when they [could] take delivery of their new Audi. Such [was] life for auto retailers and their customers across the US and Canada [when] CDK Global — a software provider to some 15,000 dealers — was waylaid by debilitating cyberattacks that began June 19 [, 2024]."[1]

[1] Kara Carlson, Evan Gorelick and Jake Bleiberg, *Car Dealers Reel From Cyberattack on $1.2 Trillion Market*, BLOOMBERG (June 21, 2024), https://www.bloomberg.com/news/articles/2024-06-21/car-dealer-chaos-arises-from-cyberattack-on-1-2-trillion-market.

2. CDK is a key software-as-a-service ("SaaS") provider for the automotive industry, providing its core product, dealer management software ("DMS"), to thousands of automotive dealerships across the United States. CDK's DMS supports automotive dealerships by providing them with essential services ranging from sales and inventory management to customer service scheduling.

3. CDK's DMS underpins virtually every element of an automotive dealership's day to-day, "generating sales leads and engaging with prospective car buyers, facilitating trade-ins, arranging auto loans, [ ] registering new vehicles . . . keep[ing] track of replacement parts, and schedul[ing] service appointments."[2] CDK even markets itself to automotive dealerships as a protector against cyberattacks.[3]

4. CDK's DMS "is 'the engine'" that drives auto retailers' operations" and the use of its DMS is far-reaching, with 2.6% of the U.S. gross domestic product contracted through CDK.

5. Despite housing vast troves of consumers' and employees' personally identifying information ("PII") on its DMS and its central role in facilitating auto dealership operations, however, CDK implemented inadequate data security measures to safeguard its DMS, leading to a massive cyberattack beginning June 18, 2024, that prompted Defendant to shutdown most of it systems.[4] When CDK attempted to restore some of its systems on June 19, 2024, Defendant suffered a second cyberattack, prompting Defendant to take its systems offline again. The

---

[2] *Id.*
[3] *Id.*
[4] *CDK Global Cyberattack Disrupts Operations at 15,000 Dealerships*, CBT NEWS (June 20, 2024), https://www.cbtnews.com/cdk-global-cyberattack-disrupts-operations-at-15000-dealerships/#:~:text=CDK%20Global%2C%20a%20major%20software%20provider%20to,shut%20down%20most%20of%20its%20systems%20temporarily.&text=%E2%80%9COut%20of%20an%20abundance%20of%20caution%20and,up%20and%20running%20as%20quickly%20as%20possible.%E2%80%9D.

sequence of cyberattacks resulted in a multi-week disruption to Defendant's DMS, crippling the automotive industry, leaving many DMS users unable to perform daily operations, forcing dealership employees to engage in pen and paper transactions, and compromising the PII of an untold number of consumers and employees that was stored in CDK's DMS (the "Data Breach").

6. CDK is well-aware of the foreseeable risks of implementing inadequate data security measures, recognizing that "cybercriminals continue to attack dealerships with ever-evolving techniques" and further recognizing ransomware and phishing attacks as the top two cybersecurity threats automotive dealerships face.[5] Indeed, CDK itself recognizes that cyberattacks in the automotive industry are on the rise with the number of automotive dealerships that have experienced a cyberattacks jumping from seventeen percent in 2023 to thirty-five percent in 2024.[6]

7. The ramifications of CDK's failure to adequately protect consumers' and its customers' employees' PII are long-lasting and severe. Armed with the PII compromised in the Data Breach, cybercriminals can and have committed a variety of crimes, including, by way of example: opening new financial accounts in Class Members' names; committing financial theft; taking out loans in Class Members' names; using Class Members' information to obtain government benefits; and using the Class Members' PII to target them with phishing and other hacking intrusions.

8. As a result of the CDK's implementation of inadequate data security measures, Plaintiffs and Class Members have now been exposed to a present injury in the form of actual misuse of their PII and have further been exposed to a certainly impending, substantial, heightened,

[5] *The State of Dealership Cybersecurity for Auto Dealerships 2024*, CDK (Dec. 30, 2024), https://cms.cdkglobal.com/sites/default/files/2025-01/24-8000_Cybersecurity_eBook.pdf.
[6] *Id.*

and imminent risk of financial fraud and identity theft for years to come. Plaintiffs and Class Members have, and must now and in the future, closely monitor their financial accounts, credit reports, and tax returns to secure their accounts in an effort to deter and detect identity theft and fraud.

9. In addition to these harms, CDK's failure to adequately secure its DMS ground automotive sales, leases, and servicing to a halt, while its DMS was offline, caused Employee/Consumer Plaintiffs and other employees of DMS users to lose income in the form of lost wages and lost commission from the diminished sale of goods and services.

10. Through this Consolidated Class Action Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all others similarly situated who have been impacted by the Data Breach.

PARTIES

Plaintiffs

11. Employee/Consumer Plaintiff, Eugene Baraga, is a natural person and citizen of California. He resides in San Franscisco, California where he intends to remain.

12. Consumer Plaintiff, Carol Berman, is a natural person and citizen of Florida. She resides in Palm Beach, Florida where she intends to remain.

13. Employee/Consumer Plaintiff Michael Paul Carvelli is a natural person and citizen of Pennsylvania. He resides in Beaver Falls, Pennsylvania where he intends to remain.

14. Employee/Consumer Plaintiff, Victoria Coombs, is a natural person and citizen of Florida. She resides in Daytona Beach, Florida where she intends to remain.

15. Employee/Consumer Plaintiff, Christopher Gordish, is a natural person and citizen of Pennsylvania. He resides in Moon Township, Pennsylvania where he intends to remain.

16. Consumer Plaintiff, Thomas Kallas, is a natural person and citizen of Michigan. He resides in Melford, Michigan where he intends to remain.

17. Employee/Consumer Plaintiff, Dustin Leeberg, is a natural person and citizen of Idaho. He resides in Coeur d'Alene, Idaho where he intends to remain.

Defendant

18. Defendant, CDK Global, LLC, is a limited liability company formed under the laws of Delaware and with its principal place of business at 1950 Hassell Road, Hoffman Estates, Illinois 60169.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are over 100 putative Class members.

20. This Court has personal jurisdiction over Defendant because it is headquartered in Illinois, regularly conducts business in Illinois, and has sufficient minimum contacts in Illinois.

21. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

A. CDK Obtains, Collects, and Stores Plaintiffs' and Class Members' PII

11. CDK is an organization that provides software solutions to automotive dealerships. CDK serves over 15,000 automotive dealership locations across America and has been providing

solutions to help dealers run their businesses for 50 years.[7] CDK advertises itself to its dealership customers as being "equipped to make the ongoing investments to protect our industry from the increasing threat of cybercriminals."[8]

12. CDK's core product is its DMS for automotive dealerships which acts as the "central hub of a dealership's functional area."[9] The DMS's functional areas include sales, accounting, service, and inventory.[10] CDK works to integrate all these areas into a singular system that streamlines a dealership's overall record management.

13. CDK's DMS system supports automotive dealerships' ability to "generate sales leads and engag[e] with prospective car buyers, facilitating trade-ins, arranging auto loans and registering new vehicles."[11] CDK's DMS also helps dealerships keep "track of replacement parts and schedule service appointments."[12]

14. Altogether, CDK's comprehensive DMS streamlines automotive dealership operations by managing dealership functions, including car sales, service scheduling, oil changes, repairs and more. Additionally, CDK's DMS enables employees to clock in and out of their shifts.

15. A dealer management system, such as CDK's DMS, stores and manages comprehensive consumer information, including consumers' contact information such as names, addresses, phone numbers, email addresses; details of vehicle purchases, including make model,

---

[7] *Who We Are*, CDK, https://www.cdkglobal.com/about (last visited Mar. 11, 2025).
[8] *Trust Center,* CDK, https://www.cdkglobal.com/cdk-trust-center (last visited Mar. 11, 2025).
[9] *What to Look for When Choosing a Dealer Management System*, CDK, https://www.cdkglobal.com/insights/what-look-when-choosing-dealer-management-system (last visited Mar. 11, 2025)
[10] *Id*.
[11] Craig Trudell, *How a Cyberattack Took 15,000 Car Dealers Offline: QuickTake*, BLOOMBERG (June 24, 2024), https://www.bloomberg.com/news/articles/2024-06-24/cdk-cyberattack-what-is-it-who-is-responsible-and-what-s-the-fallout?.
[12] *Id*.

year, and purchase date; service records, including repairs performed and parts purchased; and credit information such as current and past employers, income history, and Social Security numbers. This information is directly/indirectly entrusted to CDK by consumers, including Plaintiffs, during vehicle sales and leases and service transactions with CDK's clients.

16. In the ordinary course of providing its DMS to automotive dealerships, CDK is entrusted with, and stores, large swaths of valuable PII, including the PII of Plaintiffs and Class Members. For example, during a vehicle sale transaction, consumers' PII, including names, dates of birth, current and prior addresses, current and past employers, and Social Security numbers are input into CDK's DMS. Similarly, automotive dealerships nationwide enter their employees' PII into CDK's DMS.

17. CDK's collection and storage of Plaintiffs' and Class Members' PII in turn gives rise to equitable and legal duties to safeguard such PII from unauthorized access and compromise.

18. CDK recognizes the importance of maintaining adequate data security measures for its DMS stating that "Cybersecurity Is a Business Priority."[13] CDK purports that "we are well equipped to make the ongoing investments to protect our industry from the increasing threat of cybercriminals"[14] and claims to have implemented "a comprehensive data protection protocol that follows the NIST framework, which involves working with leading third-party industry experts and utilizing their security technologies."[15]

19. CDK further highlights its data security to its potential dealership customers, promising automotive dealerships that Defendant: (1) "secure[s] your data to protect your

[13] *Stop Cyberattacks in Their Tracks,* CDK, https://www.cdkglobal.com/dealership-operations/cybersecurity (last visited Apr. 7, 2025).
[14] *Trust Center*, CDK, https://www.cdkglobal.com/cdk-trust-center (last visited Apr. 15, 2025).
[15] *Id*.

customers against identity theft and keep them coming back to your dealership;" (2) "safeguard[s] your dealership against cyberattacks to keep your computers from slowing down or stopping altogether; and (3) "provide[s] robust cybersecurity so you can stay focused on customers and selling cars."[16]

20. Aware of how important data security is to both automotive dealerships and consumers, CDK publishes a yearly white paper entitled *The State of Dealership Cybersecurity*. In its 2024 edition, CDK recognizes that "cyber-attacks continue to plague dealerships with ever-evolving techniques" and stresses the importance of cybersecurity to automotive dealerships stating that it is "crucial to protect your data from ransom demands, reputational harm, and IT-related business disruptions." [17]

21. CDK offers itself as a data security solution to the cybersecurity risks faced by automotive dealerships, representing that "[o]ur team assists dealers so they can focus on selling vehicles and servicing their customers by providing reliable, trusted and secure solutions that help reduce expenses, protect against cyberthreats and increase productivity."[18]

22. Given the compilation of the data that CDK collected and stored, Defendant had a duty and responsibility to maintain adequate data security to safeguard the PII in its DMS. Despite these duties, however, CDK implemented inadequate data security to safeguard Plaintiffs' and Class Members' PII and to secure its DMS.

---

[16] *Stop Cyberattacks in Their Tracks,* CDK, https://www.cdkglobal.com/dealership-operations/cybersecurity (last visited Apr. 7, 2025).
[17] *The State of Dealership Cybersecurity for Auto Dealerships 2024*, CDK (Dec. 30, 2024), https://cms.cdkglobal.com/sites/default/files/2025-01/24-8000_Cybersecurity_eBook.pdf.
[18] *Id.*

B. The Data Breach

23. Notwithstanding the promised safeguards and reassurances that its cybersecurity systems were adequately maintained, a ransomware gang, BlackSuit, launched a successful and significant ransomware attack against CDK that compromised Defendant's DMS and disrupted automobile dealership operations across the country.

24. BlackSuit is a new "cybercriminal team" that is a byproduct of the Russian cybergang RoyalLocker.[19] To date, BlackSuit has hacked 95 organizations globally and they are known for engaging in "double extortion" tactics. A double extortion consists of the hackers stealing "a victim organization sensitive data, lock[ing] up its system, and also threaten[ing] to leak information."[20]

25. Beginning on June 18, 2024, BlackSuit infiltrated CDK's systems, encrypting files and disrupting CDK's core operations and services. In response to the attack, CDK made the decision to shut down its IT systems on June 19, 2024 to contain the spread of the ransomware attack. This resulted in widespread outages of its DMS for automotive dealerships.

26. While CDK initially restored services for a few hours on June 19, 2024, BlackSuit was able to successfully launch an additional attack due to CDK's inadequate security measures and response, prompting CDK to take its IT system offline again.[21] As a result, CDK's DMS remained offline until July 6, 2024.[22]

---

[19] *Explainer: The 'BlackSuit' hacker behind the CDK Global attack hitting US car dealers*, Reuters (June 27, 2024), https://www.reuters.com/technology/cybersecurity/blacksuit-hacker-behind-cdk-global-attack-hitting-us-car-dealers-2024-06-27/ (last visited Mar. 12, 2025).
[20] *Id*.
[21] Craig Trudell, *CDK Hackers Want Millions in Ransom to End Car Dealership Outage*, BLOOMBERG (June 21, 2024), https://www.bloomberg.com/news/articles/2024-06-21/cdk-hackers-want-millions-in-ransom-to-end-car-dealership-outage.
[22] Mary Walrath-Holdridge, Kinsey Crowley, & Bailey Schultz, *CDK Global cyberattack: See timeline of the hack, outages and when services could return*, USA TODAY (July 3, 2024),

27. Following the Data Breach, BlackSuit demanded a $25 million ransom payment to end the cyberattack, with news outlets reporting that CDK ultimately paid the demanded ransom.[23]

28. Following the ransom payment, CDK used a "phased restoration approach" to bring its systems back online which prioritized "critical systems and gradually bring[] additional applications online."[24] CDKs operations were ultimately restored on July 6, 2024.

29. While CDK's DMS was offline during the Data Breach, car dealerships not only had to use extreme caution when receiving communication from CDK (because bad actors were posing as Defendant to phish dealerships and their employees), but dealerships were also forced to revert to handwriting orders for customers.[25]

30. Indeed, because of the cyberattack, dealerships could not access records, complete transactions, handle orders for repairs, or schedule appointments via CDK's DMS.[26]

31. The impact of the Data Breach cannot be overstated. Based on June 2024 sales data, an accounting firm, Anderson Economic Group, LLC ("AEG"), the estimated loss to franchised dealers in the three calendar weeks of June 16 – July 5, 2024 reached $1.02 billion.[27] The $1.02

---

https://www.usatoday.com/story/money/2024/07/03/cdk-global-cyberattack-timeline/74292877007/.

[23] Sean Lyngaas, *How Did the Auto Dealer Outage End? CDK almost certainly paid a $25 million ransom*, CNN (July 11, 2024) https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html#:~:text=The%20ransom%20payment%20of%20$25,the%20company%20planned%20to%20pay.

[24] *Id*.

[25] Wyatte Grantham-Phillips, *Car Dealerships in North America revert to pens and paper after cyberattacks on software provider*, AP NEWS (June 24, 2024), https://apnews.com/article/car-dealerships-cyberattack-cdk-outage-3f7c81f6be0e212172b33cdc9f49feba.

[26] *CDK Ransomware Breach: What You Need to Know*, NGUARD (July, 3, 2024), https://nguard.com/sa-cdk-ransomware-breach-what-you-need-to-know/.

[27] *Dealer Losses Due to CDK Cyberattack Reach $1.02 Billion*, ANDERSON ECONOMIC GROUP (July 15, 2024), https://www.andersoneconomicgroup.com/dealer-losses-due-to-cdk-cyberattack-reach-1-02-billion/.

billion losses consist of: lost earnings from the approximately 56,200 new unit sales that AEG estimated were lost during the three-week period, lost earnings on used car sales, lost earnings on parts and service, additional staffing and IT service costs, and additional floor plan interest costs on inventory. It excludes damages to consumers, reputational damages to dealers, litigation costs, and multiple other categories of damages.[28]

32. As a result of the Data Breach J.D. Power and GlobalData forecast U.S. retail sales across all automakers for June 2024 to be 5.4 percent lower than they were in June 2023.[29]

33. In addition to the economic consequences for dealerships and their employees, the Data Breach had a devastating impact on dealership consumers. During the Data Breach, BlackSuit gained access to and exfiltrated files from CDK's systems that contained consumers' PII. CDK has indicated that the compromised PII includes, *inter alia*, consumers' names, addresses, and Social Security Numbers.[30]

34. CDK's sample form notification letter provided the following description:

> On June 19, 2024, CDK discovered a cyber incident where a third party gained unauthorized access to CDK's systems. Upon learning of the incident, CDK promptly launched an investigation into the matter with the assistance of data forensic experts. The investigation has now concluded. Through the investigation, CDK determined that the third party obtained a copy of certain files containing information relating to vendors of CDK/its corporate predecessor.[31]

35. While CDK purportedly took steps to contain the Data Breach, *i.e.*, paid the threat actors a likely ransom to ensure the stolen information's destruction or otherwise end the

---

[28] *Id*.
[29] Jamie L. LaReau, *CDK Cyberattack Expected to Cost Car Dealers more than $1 Billion, Michigan study says,* DETROIT FREE PRESS (July 15, 2024), https://www.freep.com/story/money/cars/2024/07/15/cdk-cyberattack-cost-car-dealerships/74408247007/.
[30] *Notice Letter*, OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL, https://www.mass.gov/doc/2024-1703-cdk-global-llc/download (last visited Apr. 8, 2024).
[31] *Id*.

ransomware attack, cyber criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[32]

36. Indeed, CDK cannot reasonably maintain that the acquired data has been destroyed and will not be further disseminated. The stolen PII is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[33]

37. Defendant's own notice to impacted individuals advises them to remain vigilant for incidents of fraud and identity theft, take further actions such as monitoring their own credit records, and notify their banks or financial institutions involved and law enforcement authorities of any suspicious activity. Recognizing the risks of the Data Breach, CDK further provided individuals with twenty-four (24) months of credit monitoring services.[34]

38. Ultimately, CDK's failed efforts to adequately safeguard Consumers' and Employee/Consumers' PII subjects Plaintiffs and members of the Class(es) to ongoing harm. When cybercriminals gain unauthorized access to Plaintiffs' information (as happened here), Plaintiffs have been and remain subject to harm such as: opening new financial accounts in Class

---

[32] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/.
[33] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, HIPAA JOURNAL (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/#:~:text=While%20ransomware%20groups%20usually%20remove,little%20incentive%20to%20delete%20it.
[34] *Notice Letter,* https://www.mass.gov/doc/2024-1703-cdk-global-llc/download.

Members' names; committing financial theft; taking out loans in Class Members' names; using Class Members' information to obtain government benefits; and using the Class Members' PII to target them with phishing and other hacking intrusions.

C. CDK Knew the Risks of Storing Plaintiffs' and Class Members' PII and the Harm to Plaintiffs and Class Members as a Result of the Data Breach was Foreseeable and Preventable

39. CDK was well aware that the highly sensitive PII which it acquires is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

40. CDK also knew that a breach of its computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

41. These risks are not theoretical, numerous high-profile breaches have occurred at third-party service providers, such as Progress Software, Fortra, and Accellion in recent years.

42. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[35] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

43. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

44. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses,

[35] *What To Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

and government entities. In 2023, there were 3,205 publicly disclosed data compromises, affecting over 353 million victims. The U.S. specifically saw a 72% increase in data breaches from the previous all-time high in 2021 and a 78% increase over 2022.[36]

45. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased in recent years. For instance, in 2019, roughly 3.5 million people reported some form of identity theft, fraud, or other consumer complaint compared to 5.4 million people in 2023.[37]

46. CDK was also well aware of the foreseeability of a cyberattack such as the Data Breach.

47. Automotive dealers have become an attractive target in part because the data they possess represents a "treasure of information," including large amounts of personal data related to financial and credit applications, customer financial information, and home addresses.[38]

48. CDK's own research recognizes that auto dealerships are increasingly concerned with cybersecurity in the face of an alarming rise in cyber-attacks. Indeed, CDK's research reveals that while ninety percent of dealerships are concerned about cybersecurity, fifty-three percent of

[36] *2023 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.
[37] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts (last visited Apr. 8, 2025).
[38] *Acting with urgency against the cyber threats to auto dealers*, ZURICH, https://www.zurichna.com/-/media/project/zwp/zna/knowledge/docs/acting-with-urgency-against-cyber-threats.pdf (last visited Apr. 8, 2025).

dealers being confident about their current cybersecurity protections, and seventeen percent of dealerships experienced a cyberattack or incident in 2023.[39]

49. The following year, CDK echoed this belief in its *The State of Dealership Cybersecurity 2024*, which stated, "it is crucial to protect your data from ransom demands, reputational harm and IT-related business disruption."[40] CDK further expressed that dealerships should not "be fooled into thinking 'it won't happen to our dealership.' All dealerships are targets and need to be protected." [41]

50. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

51. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

52. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

---

[39] *Driving Into Danger: CDK Global 2023 Cybersecurity Report Reveals Rise in Auto Dealership Cyberattacks*, CDK (Oct. 23, 2023), https://www.cdkglobal.com/media-center/driving-danger-cdk-global-2023-cybersecurity-report-reveals-rise-auto-dealership.
[40] *The State of Dealership Cybersecurity for Auto Dealerships 2024*, CDK (Dec. 30, 2024), https://cms.cdkglobal.com/sites/default/files/2025-01/24-8000_Cybersecurity_eBook.pdf.
[41] *Id*.

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[42]

53. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

54. **Driver's License Numbers—**are highly sought after by cyber criminals on the dark web because they are unique to a specific individual and extremely sensitive. This is because a driver's license number is connected to an individual's vehicle registration, insurance policies, records on file with the respective state's department of motor vehicles, places of employment, doctor's offices, government agencies, and other entities.

55. For these reasons, driver's license numbers are highly sought out by cyber criminals because they are one of the most valuable pieces of information to facilitate identity theft and fraud. This information is valuable because cyber criminals can use this information to open credit

[42] *Identify Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN. (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf.

card accounts, obtain insurance policies and submit fraudulent claims, open cell phone contracts, file fraudulent tax returns, file unemployment applications, as well as obtain bank loans under a person's name.

56. Further, unlike credit or debit card numbers in a payment card data breach, which can quickly be frozen and reissued in the aftermath of a breach, the type of PII at stake here—unique driver's license numbers—cannot be easily replaced. The ramifications of CDK's failure to keep Plaintiffs' and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

57. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[43]

22. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Indeed, even when cybercriminals do not gain access to a complete set of an individual's PII during a data breach, they can monetize the PII they did steal on the dark web to fraudsters seeking to create a full identity profile.[44] The fraudster-purchasers can then use that

[43] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (Apr. 2021), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf.
[44] Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion (last visited Mar. 6, 2025).

information to conduct various types of identity theft, such as filing a fake tax return or opening a financial account while impersonating the victim.[45]

58. When cybercriminals cross-reference two or more sources of PII and marry the stolen data from various sources, they can create complete and accurate dossiers on unsuspecting individuals. These dossiers are known as "Fullz" packages.

59. The development of Fullz packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information (such as emails, phone numbers, or credit card numbers) is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

60. Importantly, once a cybercriminal has a Fullz package, they can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[46] Most problematic, however, is that cybercriminals in possession of a Fullz package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[47]

61. Importantly, credit reports, such as those run through CDK's DMS contain Fullz-like packages as credit reports contain an individual's name, current and former addresses, birth date, Social Security number, and other information including details on an individual's current and historical credit accounts.

---

[45] *Id*.
[46] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DATADOME (Mar. 3, 2024), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.
[47] *Protection Against Fullz and Fraud*, INTEGRITY (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

62. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[48]

63. As a technology company that deals exclusively in data storage and processing, CDK was uniquely positioned to ensure the safety of its DMS and the PII stored on its platform. Yet, it failed to do so.

64. CDK also knew or should have known the importance of safeguarding its DMS, the PII stored on its platform, and of the foreseeable consequences if its data security systems were breached. CDK failed to take adequate cybersecurity measures to prevent the Data Breach.

D. CDK Maintained Inadequate Data Security Measures to Secure its DMS

65. Data disclosures and data breaches are preventable.[49] As Lucy Thompson wrote in the *Data Breach and Encryption Handbook*, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[50] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised [.]"[51]

66. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures …. Appropriate information

[48] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.
[49] Lucy L. Thompson, *Despite the Alarming Trends, Data Breaches Are Preventable*, *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[50] *Id.* at 17.
[51] *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[52]

67. CDK could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiffs and Class Members.

68. CDK's negligence in affirmatively mishandling its data security, instituting inaccurate security controls, and improperly maintaining and safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like CDK to protect and secure sensitive data they possess.

69. Despite the prevalence of public announcements of data breach and data security compromises, CDK took insufficient steps to protect the PII of Plaintiffs and Class Members.

70. While the specific details about the vulnerabilities leading to the Data Breach have not yet been publicly disclosed, BlackSuit was able to leverage weaknesses in CDK's systems that allowed cybercriminals to gain access to and ultimately encrypt CDK's systems.

71. For instance, it is suspected that BlackSuit employed a combination of phishing attacks, in which the cybercriminals targeted CDK employees into tricking them into divulging access credentials or clicking on a malicious link that enabled the cybercriminals to install malware on CDK's systems, and the exploitation of other vulnerabilities to gain initial access to CDK's systems.[53]

72. Phishing is a type of cyberattack used to trick individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source.[54]

---

[52] *Id.* (emphasis added).
[53] Yair Divinsky, *Unraveling the CDK Global Cyber attack*, VULCAN (June 30, 2024), https://vulcan.io/blog/unraveling-the-cdk-global-cyber-attack/.
[54] *Phishing*, HHS (Feb. 2018), https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf.

73. Importantly, phishing attacks are highly preventable because they rely on duping an employee into thinking that the email was legitimate. For this reason, organizations with reasonable and adequate cybersecurity will employ a secure email gateway or spam filter. This first layer of defense analyzes all inbound and outbound emails for malicious content, spam, and junk mail. Phishing protection is provided by analyzing the headers of emails and blocking known malicious IP addresses and ensuring that the sender of emails is authorized to the use the email address/domain. Secure email gateways further assess the content of emails for keywords indicative of phishing emails and follow hyperlinks in emails to identify malicious websites.

74. Organizations with reasonable and adequate cybersecurity will also implement effective training programs to educate employees not only about the dangers of phishing emails, but also how to recognize the signs that an email may be fraudulent. For example, hackers typically send phishing emails from domain names that are similar, but not identical, to the company's actual domain name.

75. Similarly, CDK's virtual private network ("VPN") infrastructure left Defendant vulnerable to attack. CDK relies on automotive dealers connecting to its "data center" via a VPN infrastructure. CDK utilizes an "always-on" VPN connection, in which a VPN connection is established between a CDK customer and CDK automatically, with no user interaction. Given the number of VPN access points (15,000 dealerships using CDK's DMS), cybercriminals could have relied on infostealer malware on a compromised dealership computer to steal user credentials and pivot into CDK's own systems.[55]

[55] Yair Divinsky, *Unraveling the CDK Global Cyber attack*, VULCAN (June 30, 2024), https://vulcan.io/blog/unraveling-the-cdk-global-cyber-attack/.

76. Finally, it appears that CDK's systems relied on outdated legacy systems and/or servers. Articles have reported that CDK's systems "integrated outdated technologies and had not seen significant upgrades for decades. This created security gaps and inefficiencies, leaving it vulnerable to attacks. The system's age, lack of innovation, outdated security protocols, inadequate backup and recovery plans, single points of failure, and fragmented infrastructure" all led to the Data Breach.[56]

77. To prevent and detect unauthorized cyber-attacks, such as the Data Breach, the Federal Bureau of Investigation recommends the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

[56] Anne-Marie Avalon, *Did Outdated Technology Burn CDK in Their Recent Cyber Attack*, AKEYLESS (July 8, 2024), https://www.akeyless.io/blog/did-outdated-technology-burn-cdk-in-their-recent-cyber-attack/.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop Protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[57]

78. Upon information and belief, CDK instituted inadequate security controls and products and/or failed to institute the controls and products that would prevent the Data Breach, including those security controls and products recommended by the FBI.

79. Further, to prevent ransomware attacks, the United States Cybersecurity & Infrastructure Security Agency recommends the following measures:

a. **Ensure your organization has a comprehensive asset management approach.** The organization should understand and take inventory of the organization's IT assets, logical (e.g., data, software) and physical (e.g., hardware). Know which data or systems are most critical for health and safety, revenue generation, or other critical services, and understand any associated interdependencies.

b. **Apply the principle of least privilege to all systems and services.** Users only have the access they need to perform their jobs. These restrictions should include: restricting user permissions to install and run software applications; restricting user/role permissions to access or modify cloud-based resources; limiting actions that can be taken on customer-managed keys by certain users/roles; blocking local accounts from remote access by using group policy to restrict network sign-in by local accounts; controlling and limiting local administration; creating an Audit Active Directory (AAD) for excessive privileges on accounts and group memberships.

[57] *Id.* at 3-4.

c. **Ensure that all hypervisors and associated IT infrastructure, including network and storage components, are updated and hardened.** Emerging ransomware strategies have begun targeting VM ware ESXi servers, hypervisors, and other centralized tools and systems, which enables fast encryption of the infrastructure at scale.

d. **Leverage best practices and enable security settings in association with cloud environments, such as Microsoft Office 365.** This includes: reviewing the shared responsibility model for cloud and ensuring you understand what makes up customer responsibility when it comes to asset protection; backing up data often; offline or cloud-to-cloud backups; enabling logging on all resources and setting alarms for abnormal usages; enabling delete protection or object lock on storage, file storage, and block storage to prevent data from being deleted.

e. **Mitigating the malicious use of remote access and remote monitoring and management (RMM) software.** This includes: auditing remote access tools on your network to identify current or authorized RMM software; reviewing logs for execution of RMM software to detect abnormal use, or RMM software running as a portable executable; using security software to detect instances of RMM software only being loaded in memory; requiring authorized RMM solutions only to be used from within your network over approved remote access solutions, such as VPNs or virtual desktop interfaces (VDIs); blocking both inbound and outbound connections on common RMM ports and protocols at the network perimeter.

f. **Employ logical or physical means of network segmentation by implementing ZTA and separating various business units or departmental resources.** This can help contain the impact of any intrusion affecting your organization and prevent or limit lateral movement on the part of malicious actors.

g. **Develop and regularly update comprehensive network diagram(s) that describe systems and data flows within your organization's network(s).** This step helps incident responders understand where to focus their efforts.

h. **Conduct regular assessments.** This ensures processes and procedures are up to date and can be followed by security staff and end users.

i. **Enable tracking prevention.** This limits the vectors that ad networks and trackers can use to track user information.[58]

80. Upon information and belief CDK instituted inadequate security controls and products and/or failed to institute the controls and products that would prevent the Data Breach, including those security controls and products recommended by the United States Cybersecurity & Infrastructure Security Agency.

81. Given that CDK was storing consumers' and employees' PII, CDK could have and should have implemented sufficient data security controls and measures, including all of the above measures, to prevent and detect cyberattacks.

[58] *See #StopRansomware Guide*, U.S. CISA (Oct. 2023), https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf (last visited Apr. 8, 2025).

82. Upon information and belief, however, CDK improperly implemented and/or failed to implement the above-described data security measures and affirmatively mishandled the maintenance of the PII with which it was entrusted, leading to the Data Breach.

83. CDK affirmatively breached its obligations and duties to Plaintiffs and Class Members and/or was otherwise negligent because it mismanaged its data security systems and policies, failing to adequately safeguard Plaintiffs' and Class Members' Sensitive Information.

84. Upon information and belief, CDK's unlawful conduct included, but is not limited to, one or more of the following affirmative acts and/or omissions:

a. Acting unreasonably in collecting, storing, and maintaining consumers' PII and failing to exercise reasonable care in its implementation of its security systems, protocols, and practices in order to sufficiently protect the PII of Plaintiffs and Class Members;

b. Negligently designing and maintaining its data security system in a manner that failed to secure Plaintiffs' and Class Members' PII from unauthorized access;

c. Implementing inadequate security controls;

d. Implementing inadequate security products;

e. Implementing inadequate security policies, including password protection policies and use of multi-factor authentication for its clients that use its systems;

f. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

g. Failing to test and assess the adequacy of its data security system;

h. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

i. Allocating insufficient funds and resources to the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

j. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

k. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

l. Failing to implement or update antivirus and malware protection software in need of security updating;

m. Designing its systems without encryption or without adequate encryption;

n. Designing its systems in a manner that did not require clients to use multi-factor authentication or require forced password changes; and

o. Failing to comply with its own Privacy Policy;

p. Failing to comply with regulations protecting the PII at issue during the period of the Data Breach;

q. Failing to recognize in a timely manner that PII had been compromised;

r. Waiting for a month before it disclosed the Data Breach; and

s. Otherwise negligently and affirmatively mishandling Plaintiffs' and Class Members' PII provided to CDK, which in turn allowed cyberthieves to access its IT systems.

85. This Data Breach would not have occurred, and Plaintiffs' and Class Members' PII would not be in the hands of the hacker, but for CDK's mishandling of its data security.

E. CDK Failed to Comply with FTC Guidelines.

86. CDK is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

87. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[59]

88. The FTC recommends that businesses:[60]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For

[59] *Start with Security: A Guide for Business*, U.S. FEDERAL TRADE COMM'N (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 22, 2024).

[60] *Protecting Personal Information: A Guide for Business*, U.S. FEDERAL TRADE COMM'N (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 22, 2024).

example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls and settings that determine which devices and traffic get through the firewall to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown

user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

89. The FTC further recommends business take additional cybersecurity steps, which include:[61]

a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;

b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.

d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and

e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.

90. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[61] *Id.*

unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

91. Upon information and belief, CDK failed to properly implement one or more of the basic data security practices described above. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized access to and exfiltration of Plaintiffs' and Class Members' PII. CDK's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

F. The Value of PII

92. Privacy Affairs' Dark Web Price Index study recently found that a cybercriminal can successfully steal someone's identity for about $1,000.[62] Specifically, a cybercriminal can obtain: stolen online banking logins, high-quality US driver's licenses, hacked Facebook accounts, stolen credit card information, and high-quality US identification cards.

93. The PII of consumers remains of high value to criminals, as evidenced by the prices offered through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[63] According to the Dark Web Price Index for 2023, payment card details for an account balance up to $1,000 have an average market value of $70, credit card

[62] Ryan Smith, *Revealed – how much is personal information worth on the dark web?*, INSURANCE BUSINESS (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx.
[63] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

details with an account limit up to $5,000 have an average market value of $110, and stolen online banking logins with a minimum of $2000 account balance have an average market value of $60.[64]

94. A study performed by Old Dominion University identified PII as: names, emails, addresses, telephone numbers, dates and places of birth, education credentials, vehicle title numbers, and account names and user IDs.[65] The study further identified sensitive personally identifiable information (SPII) as: Social Security numbers, medical history, credit and debit card numbers, driver's license numbers, and taxpayer identification numbers, among other things.[66]

95. Further, PII continues to be an attractive target to cybercriminals for the multitude of reasons previously stated. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[67]

96. The PII at issue here demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[68]

---

[64] Miklos Zoltan, *Dark Web Price Index 2023*, PRIVACY AFFAIRS (Apr. 23, 2023), https://www.privacyaffairs.com/dark-web-price-index-2023/.

[65] Poyraz, O. I., Pinto, C. A., Bouazzaoui, S., Keskin, O., & McShane, M. (2020). *Cyber-assets at risk (CAR): The cost of personally identifiable information data breaches.* 15th International Conference on Cyber Warfare and Security, Norfolk, Virginia, March 12-13, 2020.

[66] *Id*.

[67] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[68] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Network World (Feb. 6, 2015), https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

97. In 2019, the data brokering industry was worth roughly $200 billion.[69] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[70] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[71]

98. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used.

99. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[72]

G. Plaintiffs' Experiences and Injuries

Employee/Consumer Plaintiff Eugene Baraga

100. Eugene Baraga is a former employee and customer at Porsche Marin in Mill Valley, California, which, on information and belief, uses CDK's DMS.

101. Mr. Baraga worked as an Inventory Specialist at Porsche Marin from September to December in 2023. Mr. Baraga also leased a vehicle from Porsche Marin during his employment.

---

[69] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[70] *The Personal Data Revolution*, ODE HOLDINGS, INC., https://datacoup.com/ (last visited Apr. 8, 2025).
[71] *Frequently Asked Questions*, NIELSEN, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 8, 2025).
[72] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

102. On information and belief, Employee/Consumer Plaintiff Baraga's name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

103. Thus, Defendant obtained and maintained Mr. Baraga's PII. And as a result, Mr. Baraga was injured by Defendant's Data Breach.

104. Defendant's client Porsche Marin provided Employee/Consumer Plaintiff Baraga's PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Mr. Baraga's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

105. Employee/Consumer Plaintiff Baraga reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

106. Upon information and belief, through its Data Breach, Defendant compromised Employee/Consumer Plaintiff Baraga's PII.

107. Employee/Consumer Plaintiff Baraga does not recall experiencing another Data Breach, other than the breach at issue here.

108. Employee/Consumer Plaintiff Baraga fears for his personal financial security and worries about what information was exposed in the Data Breach.

109. In the aftermath of the Data Breach, Mr. Baraga has spent substantial time researching the Data Breach, checking his bank account and credit card balances, and reviewing his credit reports. Employee/Consumer Plaintiff Baraga has spent approximately five (5) hours

performing these activities. This has caused him to experience substantial stress, anxiety, and emotional harm.

110. Because of Defendant's Data Breach, Employee/Consumer Plaintiff Baraga has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Employee/Consumer Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

111. Employee/Consumer Plaintiff Baraga suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

112. Employee/Consumer Plaintiff Baraga suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

113. Employee/Consumer Plaintiff Baraga suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Mr. Baraga's PII right in the hands of criminals.

114. Because of the Data Breach, Employee/Consumer Plaintiff Baraga anticipates spending considerable amounts of time and money to try and mitigate his injuries.

115. Today, Mr. Baraga has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Consumer Plaintiff Carol Berman

116. Consumer Plaintiff Carol Berman was a customer of Rick Case Automotive, in Fort Lauderdale, Florida, which, on information and belief, uses CDK's DMS. Ms. Berman leased a vehicle from Rick Case Automotive for three years, starting on or around January 2018.

117. On information and belief, Ms. Berman's name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

118. Thus, Defendant obtained and maintained Consumer Plaintiff Berman's PII. And as a result, Ms. Berman was injured by Defendant's Data Breach.

119. Defendant's client provided Ms. Berman's PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Ms. Berman's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

120. Consumer Plaintiff Berman reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

121. Upon information and belief, through its Data Breach, Defendant compromised Ms. Berman's PII. And upon information and belief, Consumer Plaintiff Bermans' PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

122. Consumer Plaintiff Berman does not recall experiencing another Data Breach, other than the breach at issue here.

123. Consumer Plaintiff Berman did not receive Defendant's Breach Notice. Thus, Defendant provided Ms. Berman with no opportunity to protect herself from the fallout of its Data Breach.

124. Consumer Plaintiff Berman fears for her personal financial security and worries about what information was exposed in the Data Breach.

125. Indeed, in the aftermath of the Data Breach, Consumer Plaintiff Berman experienced fraudulent charges made to her credit card. She was forced to call the credit card issuer, dispute the charges, cancel the credit card, and obtain a new card.

126. On information and belief, non-public PII stolen by BlackSuit in the Data Breach, such as Consumer Plaintiff Berman's financial account information, was needed to perform unauthorized transactions using her credit card without her authorization.

127. Concerned about additional fraud attempts and the compromise of her PII, Ms. Berman spent time meticulously reviewing her credit card and other account statements.

128. Consumer Plaintiff Berman estimates that she spent approximately ten (10) hours reviewing her account statements, reviewing her credit history, signing up for credit monitoring, freezing her credit, obtaining credit reports, researching news coverage about the Data Breach, visiting her bank to remedy the fraud, changing her passwords, obtaining a new credit card, and changing her payment card information on bill pay sites

129. In addition, in the aftermath of the Data Breach, Ms. Berman has experienced a dramatic uptick in scam calls and texts. On information and belief, Consumer Plaintiff Berman's cell phone number and other contact information was stolen by BlackSuit in the Data Breach.

130. Because of Defendant's Data Breach, Ms. Berman has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Ms. Berman's injuries are precisely the type of injuries that the law contemplates and addresses.

131. Consumer Plaintiff Berman suffered actual injury from the exposure and theft of her PII—which violates his rights to privacy.

132. Consumer Plaintiff Berman suffered actual injury in the form of the fraud outlined *supra*, and damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

133. Consumer Plaintiff Berman suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Ms. Berman's PII right in the hands of criminals.

134. Because of the Data Breach, Ms. Berman anticipates spending considerable amounts of time and money to try and mitigate her injuries.

135. Today, Consumer Plaintiff Berman has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Employee/Consumer Plaintiff Michael Paul Carvelli

136. Employee/Consumer Plaintiff Michael Paul Carvelli is an employee and customer at Lithia Motors in Moon Township, Pennsylvania, which, on information and belief, uses CDK's DMS.

137. Mr. Carvelli has held his position as Finance Manager at Lithia Motors from 2023 to present.

138. On information and belief, Mr. Carvelli's name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

139. Thus, Defendant obtained and maintained Mr. Carvelli's PII. And as a result, Mr. Carvelli was injured by Defendant's Data Breach.

140. Defendant's client Lithia Motors provided Mr. Carvelli's PII to Defendant and trusted CDK would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Mr. Carvelli's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

141. Employee/Consumer Plaintiff Carvelli reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

142. Upon information and belief, through its Data Breach, Defendant compromised Mr. Carvelli's PII. And upon information and belief, Mr. Carvelli's PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

143. Mr. Carvelli does not recall experiencing another Data Breach, other than possibly receiving a notice about the Equifax breach many years ago.

144. Mr. Carvelli fears for his personal financial security and worries about what information was exposed in the Data Breach.

145. CDK's Data Breach has caused Mr. Carvelli substantial financial and emotional hardship.

146. In his capacity as Finance Manager at Defendant's client, Mr. Carvelli relied on CDK's software to perform nearly all if his job duties. When a salesperson has a sale to finance, Mr. Carvelli obtains the customer's information, applies for loans to several lenders, and processes those loans on CDK's DMS. As a customer who has purchased cars from multiple dealerships that use CDK, Mr. Carvelli's information was entered into the CDK platform. As an employee, CDK also has his employee information. One hundred percent of Plaintiff Carvelli's pay was based

on commissions from vehicle sales at the time of the CDK outage and until very recently. (He now has a salary plus commission.)

147. When the Data Breach caused CDK's software to become inoperable, Mr. Carvelli's ability to earn commissions was greatly reduced. Mr. Carvelli, along with his colleagues, was unable to sell or lease vehicles using financing. First there were days of no sales, they could not transact any business. After that, they instituted paper and pen for about a week. Mr. Carvelli went to work, but his ability to complete financed deals was greatly curtailed. They took deposits on a few deals but had to wait for CDK to come back online to complete the transactions. Further, many customers were unwilling to finalize purchases due to the cumbersome process of using paper documents and sending them via US Mail.

148. Employee/Consumer Plaintiff Carvelli estimates he and his colleagues sold less than half of the usual volume of vehicles when CDK's software was inoperable due to the Data Breach. Even afterward, the CDK Data Breach caused a general downturn in car sales due to the loss of trust by potential customers.

149. Mr. Carvelli estimates he lost approximately forty to sixty thousand dollars ($40,000-$60,000) in income as a result of CDK's Data Breach. He earned $80,000 to $90,000 in the first six months of 2024 (before the Data Breach) and expected similar earnings in the second half (for an expected total of $160,000-180,000) but only made $120,000 for the full year of 2024 after the Data Breach suspended and damaged the market for car sales and financing.

150. In the aftermath of the Data Breach, Mr. Carvelli has spent substantial time researching and monitoring news about the Data Breach via Google, automotive news articles, and news stories. He constantly changes his passwords and monitors news about the Data Breach. At the beginning after the Data Breach, he regularly checked his bank accounts, and he continues to

monitor them directly and through Credit Karma and Experian. He has received and is very concerned about notifications that his information is on the dark web. Mr. Carvelli estimates that he has spent the equivalent of about two months through the present between researching and monitoring the Data Breach and his accounts. This has caused him to experience substantial stress, anxiety, and emotional harm. He feels constant worry, concern, and agitation; he is stressed that his information is out there and that it can affect his financial situation, so he has a lack of certainty that he can move to the next stages of life with financial confidence.

151. In addition to receiving notifications that his information is on the dark web in the aftermath of the Data Breach, Mr. Carvelli has experienced a dramatic uptick in scam calls and texts and emails. On information and belief, Mr. Carvelli's cell phone number and other contact information was stolen by BlackSuit in the Data Breach.

152. Because of Defendant's Data Breach, Mr. Carvelli has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Mr. Carvelli's injuries are precisely the type of injuries that the law contemplates and addresses.

153. Mr. Carvelli suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

154. Mr. Carvelli suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

155. Mr. Carvelli suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

156. Because of the Data Breach, Mr. Carvelli anticipates spending considerable amounts of time and money to try and mitigate his injuries.

157. Today, Mr. Carvelli has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Employee/Consumer Plaintiff Victoria Coombs

158. Employee/Consumer Plaintiff Victoria Coombs was employee of Indian Motorcycle Daytona Beach, in Daytona Beach, Florida, which, on information and belief, uses CDK's DMS. Ms. Coombs worked as an Internet Manager for Indian Motorcycle Daytona Breach from March 2024 to November 2024.

159. On information and belief, Ms. Coombs' name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

160. Thus, Defendant obtained and maintained Employee/Consumer Plaintiff Coombs' PII. And as a result, Ms. Coombs was injured by Defendant's Data Breach.

161. Defendant's client provided Plaintiff Coombs' PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Employee/Consumer Plaintiff Coombs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

162. Employee/Consumer Plaintiff Coombs reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

163. Upon information and belief, through its Data Breach, Defendant compromised Employee/Consumer Plaintiff Coombs' PII. And upon information and belief, Ms. Coombs' PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

164. Employee/Consumer Plaintiff Coombs does not recall experiencing another Data Breach, other than the breach at issue here.

165. Employee/Consumer Plaintiff Coombs did not receive Defendant's Breach Notice. Thus, Defendant provided Ms. Coombs with no opportunity to protect herself from the fallout of its Data Breach.

166. Employee/Consumer Plaintiff Coombs fears for her personal financial security and worries about what information was exposed in the Data Breach.

167. CDK's Data Breach has caused Ms. Coombs substantial financial and emotional hardship.

168. In her capacity as an Internet Manager at Defendant's client, Ms. Coombs relied on CDK's software to perform nearly all of her job duties. All of her customers' and leads' contact information was stored within CDK's software and she used the software's texting and calling feature to communicate with 30-50 leads per day and set appointments. Ms. Coombs was paid a commission per appointment made.

169. When the Data Breach caused CDK's software to become inoperable, Ms. Coombs was effectively unable to earn.

170. Without her regular income, Ms. Coombs was forced to borrow money from family members to pay her rent and pay her car payments, which she was unable to make on time. Furthermore, during the period when CDK's DMS was inoperable, Plaintiff Coombs was unable

to afford to see her therapist or psychiatrist, and was unable to afford her medication. This caused her to experience substantial stress, anxiety, and emotional harm.

171. Even when the CDK's software was restored, all of Ms. Coombs' leads' contact information was no longer available. Thus, the Data Breach affected Employee/Consumer Plaintiff Coombs ability to earn commissions for months after the Data Breach. She estimates her lost income at approximately $7,000.

172. Furthermore, in the aftermath of the Data Breach, Employee/Consumer Plaintiff Coombs received notifications from Credit Karma that a credit card had been opened in her name.

173. On information and belief, non-public PII stolen by BlackSuit in the Data Breach, such as Ms. Coombs's Social Security number, was needed to open a credit card in her name and without her authorization.

174. Employee/Consumer Plaintiff Coombs has received other notifications that her PII has been detected on the Dark Web.

175. Additionally, Ms. Coombs observed that her credit score has dropped precipitously. Ms. Coombs believes this is the result of being a victim of identity theft and fraud caused by the Data Breach.

176. Concerned about additional fraud attempts and the compromise of her PII, Employee/Consumer Plaintiff Coombs spent time researching the Data Breach, reviewing her bank accounts, and reviewing her credit reports.

177. In addition, in the aftermath of the Data Breach, Ms. Coombs has experienced a dramatic uptick in scam calls and texts and emails. On information and belief, Ms. Coombs' cell phone number credit history, and other contact information was stolen by BlackSuit in the Data Breach.

178. Because of Defendant's Data Breach, Ms. Coombs has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Ms. Coombs's injuries are precisely the type of injuries that the law contemplates and addresses.

179. Employee/Consumer Plaintiff Coombs suffered actual injury from the exposure and theft of her PII—which violates his rights to privacy.

180. Employee/Consumer Plaintiff Coombs suffered actual injury in the form of the fraud outlined *supra*, and damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

181. Employee/Consumer Plaintiff Coombs suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Ms. Coombs' PII right in the hands of criminals.

182. Because of the Data Breach, Ms. Coombs anticipates spending considerable amounts of time and money to try and mitigate her injuries.

183. Today, Ms. Coombs has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Employee/Consumer Plaintiff Christopher Gordish

184. Employee/Consumer Plaintiff Christopher Gordish is an employee and customer at Lithia Motors in Moon Township, Pennsylvania, which, on information and belief, uses CDK's DMS.

185. Mr. Gordish has held his position as a General Sales Manager at Lithia Motors for approximately three years and has worked there from 2018 to present.

186. On information and belief, Mr. Gordish's name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

187. Thus, Defendant obtained and maintained Mr. Gordish's PII. And as a result, Mr. Gordish was injured by Defendant's Data Breach.

188. Defendant's client Lithia Motors provided Mr. Gordish's PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Mr. Gordish's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

189. Employee/Consumer Plaintiff Gordish reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

190. Upon information and belief, through its Data Breach, Defendant compromised Mr. Gordish's PII. And upon information and belief, Mr. Gordish's PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

191. Mr. Gordish does not recall experiencing another Data Breach, other than the breach at issue here.

192. Mr. Gordish fears for his personal financial security and worries about what information was exposed in the Data Breach.

193. CDK's Data Breach has caused Mr. Gordish substantial financial and emotional hardship.

194. In his capacity as a General Sales Manager at Defendant's client, Mr. Gordish relied on CDK's software to perform nearly all of his job duties. Mr. Gordish runs the sales department; thus, when a salesperson sells a vehicle, he uses CDK's software to prepare documents for the sale and to finalize the sale. Approximately 60%-70% of Plaintiff Gordish's pay is based on commissions from vehicle sales.

195. When the Data Breach caused CDK's software to become inoperable, Mr. Gordish's ability to earn commissions was greatly reduced. Mr. Gordish, along with his colleagues, were unable to sell vehicles using financing, were unable to lease vehicles, and, as a result, sold many vehicles via less lucrative cash deals. Further, many customers were unwilling to finalize purchases due to the cumbersome process of using paper documents and sending them via US Mail.

196. Employee/Consumer Plaintiff Gordish estimates he and his colleagues sold less than half of the usual volume of vehicles when CDK's software was inoperable due to the Data Breach.

197. Mr. Gordish estimates he lost approximately ten thousand dollars ($10,000) in income as a result of CDK's Data Breach.

198. In the aftermath of the Data Breach, Mr. Gordish has spent substantial time researching the Data Breach, checking his bank account and credit card balances, and reviewing his credit reports. Mr. Gordish spends approximately ten (10) minutes per day monitoring his accounts. This has caused him to experience substantial stress, anxiety, and emotional harm.

199. In addition, in the aftermath of the Data Breach, Mr. Gordish has experienced a dramatic uptick in scam calls and texts and emails. On information and belief, Mr. Gordish's cell phone number and other contact information was stolen by BlackSuit in the Data Breach.

200. Because of Defendant's Data Breach, Mr. Gordish has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Mr. Gordish's injuries are precisely the type of injuries that the law contemplates and addresses.

201. Mr. Gordish suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

202. Mr. Gordish suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

203. Mr. Gordish suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's PII right in the hands of criminals.

204. Because of the Data Breach, Mr. Gordish anticipates spending considerable amounts of time and money to try and mitigate his injuries.

205. Today, Mr. Gordish has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Consumer Plaintiff Thomas Kallas

206. Consumer Plaintiff Thomas Kallas is customer of Szott Toyota in Oakland County, Michigan, and Suburban Toyota in Farmington Hills, Michigan, which, on information and belief, use CDK's DMS.

207. Mr. Kallas purchased a vehicle from Szott Toyota in January of 2022, he purchased a 2022 Toyota 4-Runner from Suburban Toyota in Farmington Hills, MI. In July of 2023, he purchased a 2024 Grand Highlander from Szott Toyota.

208. On information and belief, Consumer Plaintiff Kallas' name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

209. Thus, Defendant obtained and maintained Mr. Kallas' PII. And as a result, Mr. Kallas was injured by Defendant's Data Breach.

210. Defendant's client Szott Toyota provided Mr. Kallas' PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Kallas' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

211. Consumer Plaintiff Kallas reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

212. Upon information and belief, through its Data Breach, Defendant compromised Mr. Kallas' PII. And upon information and belief, Mr. Kallas' PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

213. Mr. Kallas' fears for his personal financial security and worries about what information was exposed in the Data Breach.

214. Indeed, in the aftermath of the Data Breach, Mr. Kallas experienced fraudulent charge made to his credit card. He was forced to call the credit card issuer, dispute the charges, cancel the credit card, and obtain a new card.

215. On information and belief, non-public PII stolen by BlackSuit in the Data Breach, such as Mr. Kallas' financial account information, was needed to perform an unauthorized transaction using his credit card without his authorization.

216. Concerned about additional fraud attempts and the compromise of his PII, Mr. Kallas spent time researching the Data Breach and meticulously reviewing his account statements and his credit reports. Mr. Kallas estimates that he has spent approximately two (2) hours per week reviewing his financial statements since the Data Breach occurred.

217. In addition, in the aftermath of the Data Breach, Mr. Kallas has experienced a dramatic uptick in scam calls, texts and emails. On information and belief, Mr. Kallas' cell phone number and other contact information was stolen by BlackSuit in the Data Breach.

218. Because of Defendant's Data Breach, Mr. Kallas has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Mr. Kallas' injuries are precisely the type of injuries that the law contemplates and addresses.

219. Consumer Plaintiff Kallas suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

220. Consumer Plaintiff Kallas suffered additional actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

221. Consumer Plaintiff Kallas suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Mr. Kallas' PII right in the hands of criminals.

222. Because of the Data Breach, Plaintiff Kallas anticipates spending considerable amounts of time and money to try and mitigate his injuries.

223. Today, Consumer Plaintiff Kallas has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Employee/Consumer Plaintiff Dustin Leeberg

224. Employee/Consumer Plaintiff Dustin Leeberg is an employee and customer of Findlay Auto Group, in Post Falls, Idaho which, on information and belief, uses CDK's DMS.

225. Mr. Leeberg has held his position as a salesman at Findlay Auto Group from May 2023 to present.

226. Additionally, Mr. Leeberg purchased a vehicle from Evergreen Chevrolet in Issaquah, Washington.

227. On information and belief, Mr. Leeberg's name, address, date of birth, phone number, credit history, driver's license, and Social Security number were stored within CDK's systems at the time of the Data Breach.

228. Defendant's client provided Mr. Leeberg's PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Mr. Leeberg's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

229. Employee/Consumer Plaintiff Leeberg reasonably understood that a portion of the funds paid to Defendant by its client would be used to pay for adequate cybersecurity and protection of PII.

230. Upon information and belief, through its Data Breach, Defendant compromised Mr. Leeberg's PII. And upon information and belief, Plaintiff Leeberg's PII has already been published—or will be published imminently—by BlackSuit on the Dark Web.

231. Mr. Leeberg does not recall experiencing another Data Breach, other than the breach at issue here.

232. Mr. Leeberg fears for his personal financial security and worries about what information was exposed in the Data Breach.

233. CDK's Data Breach has caused Mr. Leeberg substantial financial and emotional hardship.

234. In his capacity as a sales personnel member, Mr. Leeberg relied on CDK's software to perform sales and service transactions. A substantial portion of Mr. Leeberg's pay is based on commissions from vehicle sales.

235. When the Data Breach caused CDK's software to become inoperable, Mr. Leeberg was unable to work for approximately three (3) weeks. Although his employer provided him with some compensation, Mr. Leeberg lost opportunities for income as a result of CDK's Data Breach.

236. In addition, in the aftermath of the Data Breach, in September 2024, Mr. Leeberg received a notification from Experian that his PII has been detected on the Dark Web.

237. In the aftermath of the Data Breach, Mr. Leeberg has spent substantial time researching the Data Breach, enrolling in credit monitoring, checking his bank account and credit card balances, and reviewing his credit reports. Mr. Leeberg estimates he has spent approximately thirty (300 hours performing these activities since the Data Breach.

238. In addition, in the aftermath of the Data Breach, Mr. Leeberg has experienced a dramatic uptick in scam calls and texts and emails. On one occasion, a scammer impersonating

someone from CDK attempted to induce Mr. Leeberg to provide him with his Social Security number.

239. On information and belief, Mr. Leeberg's cell phone number and other contact information was stolen by BlackSuit in the Data Breach.

240. Because of Defendant's Data Breach, Mr. Leeberg has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Mr. Leeberg's injuries are precisely the type of injuries that the law contemplates and addresses.

241. Mr. Leeberg suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

242. Mr. Leeberg suffered additional actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

243. Mr. Leeberg suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Employee/Consumer Plaintiff's PII right in the hands of criminals.

244. Because of the Data Breach, Mr. Leeberg anticipates spending considerable amounts of time and money to try and mitigate his injuries.

245. Today, Employee/Consumer Plaintiff Leeberg has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

H. The Impact of the Data Breach on Plaintiffs and Class Members

246. CDK's inadequately maintained cybersecurity measures have severe and long-lasting ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, date

of birth, addresses, and Social Security Numbers—hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, the Plaintiffs have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach. The Employee/Consumer subclass have suffered additional injury in the form of lost income due to the Data Breach.

247. As discussed above, the PII exposed in the Data Breach is highly coveted and valuable on underground markets as it can be used to commit identity theft and fraud. With access to an individual's PII, malicious actors can use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards.

248. Malicious actors can also use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities." [73]

249. Further, malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII, meaning individuals can be the victims of several cybercrimes stemming from a single data breach.

250. Victims of the Data Breach face significant harms as the result of the Data Breach, including, but not limited to, actual identity theft and fraud as well as substantial and imminent risk of identity theft and fraud. Plaintiffs and Class Members are forced to spend time, money, and effort reacting to and dealing with the fallout of the Data Breach, including purchasing credit

[73]A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

monitoring services, reviewing financial and healthcare statements, checking credit reports, and spending time and effort searching for and responding to unauthorized activity.

251. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2021 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 84% reported anxiety;
- 76% felt violated;
- 32% experienced financial related identity problems;
- 83% reported being turned down for credit or loans;
- 32% reported problems with family members as a result of the breach; and
- 10% reported feeling suicidal.[74]

252. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate/lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and

[74] *2021 Consumer Aftermath Report,* IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2021/09/ITRC_2021_Consumer_Aftermath_Report.pdf (last visited Apr. 8, 2025).

- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[75]

253. The unauthorized disclosure of sensitive PII to data thieves also reduces its inherent value to its owner, which has been recognized by courts as an independent form of harm.[76]

254. Plaintiffs are injured every time their data is stolen and traded on underground markets, even if they have been victims of previous data breaches. Indeed, the dark web is comprised of multiple discrete repositories of stolen information that can be aggregated together or accessed by different criminal actors who intend to use it for different fraudulent purposes. Each data breach increases the likelihood that a victim's PII will be exposed to more individuals who are seeking to misuse it at the victim's expense.

255. As a result of the numerous injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to the following:

a. the unconsented disclosure of confidential information to a third party;

b. losing the inherent value of their PII;

c. losing the value of access to their PII permitted by CDK;

d. identity theft and fraud resulting from the theft of their PII;

e. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

f. anxiety, emotional distress, and loss of privacy;

---

[75] *Id.*

[76] *See In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 462 (D. Md. 2020) ("Neither should the Court ignore what common sense compels it to acknowledge—the value that personal identifying information has in our increasingly digital economy. Many companies, like Marriott, collect personal information. Consumers too recognize the value of their personal information and offer it in exchange for goods and services.").

g. the present value of ongoing credit monitoring and identity theft protection services necessitated by CDK's Data Breach;

h. unauthorized charges and loss of use of and access to their accounts;

i. lowered credit scores resulting from credit inquiries following fraudulent activities;

j. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to mitigate and address the actual and future consequences of the Data Breach, including searching for fraudulent activity, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with the repercussions of the Data Breach;

k. the continued, imminent, and certainly impending injury flowing from potential fraud and identity theft posed by their PII being in the possession of one or many unauthorized third parties; and

l. the Employee/Consumer Subclass also experienced loss of income due to the Data Breach.

256. As a result of the actual and real risk of identity theft impacted consumers must, as CDK's Notice instructs, "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports we are providing (discussed below) for suspicious activity and potential errors, and to report suspected identity theft incidents

to local law enforcement or your state's attorney general" and they will most likely do this for the remainder of their lifetimes.[77]

257. Plaintiffs and Class Members have spent and will spend additional time in the future on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

258. Plaintiffs' mitigation efforts are consistent with the steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[78]

259. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement.

260. Plaintiffs and Class Members place significant value in data security. The American Bankers Association, reporting on a global consumer survey regarding concerns about privacy and data security, noted that 29% of consumers would avoid using a company that had experienced a

[77] *Notice Letter*, OFFICE OF THE MASSACHUSETTS ATTORNEY GENERAL, https://www.mass.gov/doc/2024-1703-cdk-global-llc/download (last visited Apr. 8, 2024).
[78] *See Home Page*, FTC - IDENTITY THEFT.GOV, https://www.identitytheft.gov/Steps (last visited Apr. 8, 2025).

data breach, with 63% of consumers indicating they would avoid such a company for a period of time.[79]

261. Plaintiffs and Class Members have a direct interest in CDK's promises and duties to protect their PII, *i.e.*, that CDK *not* increase their risk of identity theft and fraud.

262. Because CDK failed to live up to its promises and duties in this respect, Plaintiffs and Class Members seek the present value of ongoing identity protection services to compensate them for the present harm and present and continuing increased risk of harm caused by CDK's wrongful conduct. Through this remedy, Plaintiffs seek to restore themselves and Class Members as close to the same position as they would have occupied but for CDK's wrongful conduct, namely its failure to adequately protect Plaintiffs' and Class Members' PII.

263. Plaintiffs and Class Members further seek to recover the value of the unauthorized access to their PII permitted through CDK's wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's PII is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology.

264. Nevertheless, Plaintiffs may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer.

[79] *What Compliance Needs to Know in the Event of a Security Breach*, ABA BANKING JOURNAL (Sept. 9, 2019), https://bankingjournal.aba.com/2019/09/what-compliance-needs-to-know-in-the-event-of-a-security-breach/.

265. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and Class Members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

266. These injuries to Plaintiffs and Class Members were directly and proximately caused by CDK's failure to implement or maintain adequate data security measures for the victims of the Data Breach.

267. Further, because CDK continues to hold their PII, Plaintiffs and Class Members have an interest in ensuring that their PII is secured and not subject to further theft.

CLASS ACTION ALLEGATIONS

268. Plaintiffs bring this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure ("F.R.C.P.") on behalf of Plaintiffs and the following classes/subclass(es) (collectively, the "Class(es)"):

Nationwide Class:

"All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the Data Breach."

Nationwide Employee/Consumer Subclass:

"All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the Data Breach and who were also employees of a business impacted by the ransomware attack."

California Subclass

"All individuals residing in California whose PII was exposed to unauthorized third parties as a result of the Data Breach." (the "California Subclass").

California Employee/Consumer Subclass:

"All individuals residing in California whose PII was exposed to unauthorized third parties as a result of the Data Breach and who were also employees of a business impacted by the ransomware attack." (the "California Employee Subclass").

Florida Subclass

"All individuals residing in Florida whose PII was exposed to unauthorized third parties as a result of the Data Breach." (the "Florida Subclass").

269. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendant has a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

270. In the alternative, Plaintiffs reserve the right to request additional subclasses as necessary based on the types of PII that were compromised.

271. Plaintiffs also reserve the right to amend the above Class and Subclass definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

272. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Plaintiffs are informed and believe, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality/Predominance: Plaintiffs and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendant had a legal duty to Plaintiffs and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII;

2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

6) Whether Defendant adequately, promptly and accurately informed Plaintiffs and Class Members that their PII had been compromised;

7) How and when Defendant actually learned of the Data Breach;

8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class Members;

9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Plaintiffs' and Class Members' PII;

11) Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant's wrongful conduct;

12) Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

c. Typicality: Plaintiffs' claims are typical of the claims of the Plaintiff Classes. Plaintiffs and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Plaintiffs are adequate representatives of each of the Plaintiff Classes in that Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Plaintiffs anticipate no management difficulties in this litigation.

e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense where they to pursue individual litigation. This makes or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

273. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

274. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Classes in their entireties. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiffs' challenge of these policies and procedures hinges on Defendant's conduct concerning the Classes in their entirety, not on facts or law applicable only to Plaintiffs.

275. Unless a Class-wide injunction is issued, Defendant may continue failing to secure Class Members' PII properly, and Defendant may continue to act unlawfully, as set forth in this Complaint.

276. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under F.R.C.P. Rule 23(b)(2).

CAUSES OF ACTION

COUNT ONE
Negligence
(On behalf of Plaintiffs and the Classes)

277. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

278. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard its DMS and Plaintiffs' and Class Members' PII, and to use commercially reasonable methods to do so. Defendant took on this

obligation upon accepting and storing Plaintiffs' and Class Members' PII on its computer systems, servers, and networks.

279. CDK also owed a duty to ensure that its DMS remained secure from unauthorized access and that its services stayed operational and not experience extended outages or unavailability.

280. Among these duties, Defendant was expected:

a. to implement adequate data security measures to guard against cyberattacks, and taking other reasonable security measures to safeguard and adequately secure its DMS from unauthorized access;

b. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

c. to protect Plaintiffs' and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

d. to implement processes to detect the Data Breach quickly and to act on warnings about data breaches timely;

e. to promptly notify Plaintiffs and Class Members of any data breach, security incident or intrusion that affected or may have affected their PII, and

f. to promptly and effectively respond to and restore the dealership operating systems which were wholly dependent upon Defendant's computer systems, software, servers, and related equipment.

281. Defendant knew or should have known that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care to not subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

282. Defendant knew or should have known of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, that a cyberattack would or could

otherwise impair the operations of its DMS, and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

283. Defendant knew or should have known that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII or adequate protect the operations of its DMS.

284. Only Defendant was in the position to ensure that its systems and protocols were sufficient guard against cyberattacks, disruptions to its DMS's operations, and to protect the PII that Plaintiffs and Class Members had entrusted to it.

285. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard its DMS and their PII and by failing to promptly and effectively respond to and restore the dealership operating systems which were wholly dependent upon Defendant's computer systems, software, servers, and related equipment.

286. Because Defendant knew that a breach of its systems could damage numerous individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its DMS and the PII stored thereon.

287. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant could protect its systems and the PII it stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

288. Defendant also had independent duties that required Defendant to reasonably safeguard its DMS and Plaintiffs' and Class Members' PII and promptly notify them about the

Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiffs, and/or the remaining Class Members.

289. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. Implementing inadequate data security measures to safeguard its DMS;

b. by failing to provide fair, reasonable and/or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII;

c. by failing to timely and accurately disclose that Plaintiffs' and Class Members' PII had been improperly acquired or accessed;

d. by failing to adequately protect and safeguard PII by knowingly disregarding standard information security principles, despite obvious risks and by allowing unmonitored and unrestricted access to unsecured PII;

e. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather Plaintiffs' and Class Members' PII, misuse the PII and intentionally disclose it to others without consent;

f. by failing to adequately train its employees not to store PII longer than absolutely necessary;

g. by failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' PII;

h. by failing to implement processes to quickly detect data breaches, security incidents or intrusions;

i. by failing to encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats, and

j. by failing to promptly and effectively respond to and restore the dealership operating systems which were wholly dependent upon Defendant's computer systems, software, servers, and related equipment.

290. Defendant's willful failure to abide by these duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

291. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harm and damages (as alleged above).

292. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiffs and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

293. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access after learning of the Data Breach by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach. To date, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class Members.

294. Further, explicitly failing to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII and access their medical records and histories.

295. There is a close causal connection between Defendant's failure to implement security measures to protect its DMS and Plaintiffs' and Class Members' PII and the harm incurred (or risk of imminent harm suffered) by Plaintiffs and Class Members. Plaintiffs' and Class Members' PII was accessed, and Employee/Consumer Plaintiffs lost commission, the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing and maintaining appropriate security measures.

296. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

297. Plaintiffs and Class Members have suffered and will continue to suffer damages as the direct and proximate result of Defendant's negligent conduct, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PII, (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received; and (ix) for the Employee Subclasses, lost commission-based and bonus income resulting from Defendant's failure to promptly and effectively respond to and restore its DMS, which dealership employees were wholly dependent upon Defendant's computer systems, software, servers, and related equipment to perform their job responsibilities.

COUNT TWO
Negligence *Per Se*
(On behalf of Plaintiffs and the Classes)

298. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

299. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits companies such as Defendant from "using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce," including failing to use reasonable measures to protect PII. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

300. In addition to the FTC rules and regulations and state law, other states and jurisdictions where victims of the Data Breach are located require that Defendant protect PII from unauthorized access and disclosure and timely notify the victim of a data breach, including, but not limited to, under the Illinois Consumer Fraud and Deceptive Business Practices Act 815 ICLS 505/1, *et seq*., the California Consumer Privacy Act - Cal. Civ. Code § 1798.150(a), and the Florida Deceptive and Unfair Trade Practices Act - Fla. Stat. § 501.201, *et seq.*

301. Defendant violated FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a Data Breach and the exposure of Plaintiffs' and Class Members' highly sensitive PII.

302. Each of Defendant's statutory violations of Section 5 of the FTC Act and other applicable statutes, rules and regulations, constitute negligence *per se*.

303. Plaintiffs and Class Members are within the category of persons the FTC Act were intended to protect.

304. The harm that occurred because of the Data Breach described herein is the type of harm the FTC Act was intended to guard against.

305. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PII, (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received; and (ix) for the Employee/ Subclasses, lost commission-based and bonus income resulting from Defendant's failure to promptly and effectively respond to and restore its DMS, which dealership employees were wholly dependent

upon Defendant's computer systems, software, servers, and related equipment to perform their job responsibilities.

COUNT THREE
Breach of Confidence
(On behalf of Plaintiffs and the Classes)

306. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

307. During Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential nature of the PII that Plaintiffs and Class Members provided to it.

308. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by promises and expectations that Plaintiffs and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

309. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

310. Plaintiffs and Class Members also provided their PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting its networks and data systems.

311. Defendant voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

312. Due to Defendant's failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class Members' confidence and without their express permission.

313. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages, as alleged herein.

314. But for Defendant's failure to maintain and protect Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. The Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class Members' PII and the resulting damages.

315. The injury and harm Plaintiffs and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendant's unauthorized misuse of Plaintiffs' and Class Members' PII. Defendant knew its data systems and protocols for accepting and securing Plaintiffs' and Class Members' PII had security and other vulnerabilities that placed Plaintiffs' and Class Members' PII in jeopardy.

316. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PII, (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received; and (ix) for the Employee Subclasses, lost commission-based and bonus income resulting from Defendant's failure to promptly and effectively respond to and restore its DMS, which dealership employees were wholly dependent upon Defendant's computer systems, software, servers, and related equipment to perform their job responsibilities .

COUNT FOUR
Breach of Implied Contract
(On behalf of Plaintiffs and the Classes)

317. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

318. Through their course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

319. CDK required Plaintiffs and Class Members to provide, or authorize the transfer of, their PII in order for OTP to provide services. In exchange, CDK entered into implied contracts with Plaintiffs and Class Members in which CDK agreed to implement adequate data security measures to protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

320. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

321. As a condition of being employees and/or customers of Defendant's clients, Plaintiffs and Class Members provided and entrusted their PII to Defendant. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

322. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

323. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

324. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised because of the Data Breach.

325. Every contract in has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

326. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

327. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members, and continued acceptance of PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

328. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

329. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered and will continue to suffer injury, as alleged herein, including but not limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how

to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PII, (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received; and (ix) for the Employee Subclasses, lost commission-based and bonus income resulting from Defendant's failure to promptly and effectively respond to and restore its DMS, which dealership employees were wholly dependent upon Defendant's computer systems, software, servers, and related equipment to perform their job responsibilities.

330.

COUNT FIVE
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Classes)

331. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

332. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by CDK and that was ultimately accessed or compromised in the Data Breach.

333. As a business that provides dealership management software essential to the dealerships, CDK accepts and stores the PII of its clients' employees and customers, giving rise to a fiduciary duty to Plaintiffs and Class Members. In light of this fiduciary relationship, CDK must act primarily for the benefit of its clients' employees and customers, which includes safeguarding

and protecting Plaintiffs' and Class Members' PII, even in the absence of direct privity between them.

334. Because of that fiduciary duty, Plaintiffs and Class Members either directly or indirectly gave CDK their PII in confidence, believing that CDK would protect that information. Plaintiffs and Class Members would not have provided CDK with this information had they known it would not be adequately protected.

335. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became the guardian of Plaintiffs' and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII to act primarily for Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs' and Class Members' PII, (ii) to timely notify Plaintiffs and Class Members of a data breach and disclosure, and (iii) to maintain complete and accurate records of what information (and where) Defendant did has and continues to store.

336. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its customers' employees and customers—in particular, to keep their PII secure.

337. Defendant breached its fiduciary duties to Plaintiffs and Class Members failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' PII, failing to comply with the data security guidelines set forth by the FTC, otherwise failing to safeguard the PII of Plaintiffs and Class Members it collected, and failing to provide notice of the Data Breach in a reasonable and practicable period of time.

338. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not

limited to: (i) actual identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Class Members' PII in its continued possession, (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, (vii) the diminished value of Plaintiffs' and Class Members' PII, (viii) the diminished value of Defendant's services for which Plaintiffs and Class Members paid and received; and (ix) for the Employee/Consumer Subclasses, lost commission-based and bonus income resulting from Defendant's failure to promptly and effectively respond to and restore its DMS, which dealership employees were wholly dependent upon Defendant's computer systems, software, servers, and related equipment to perform their job responsibilities.

339. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT SEVEN
Unjust Enrichment
(On behalf of the Plaintiffs and the Classes)

340. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

341. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by CDK and was ultimately accessed or compromised in the Data Breach.

342. Upon information and belief, Defendant funds its data-security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

343. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendant.

344. The relationship between CDK and Plaintiffs and Class Members is not attenuated, as Plaintiffs and Class Members had a reasonable expectation that the security of their PII would be maintained when they provided their PII to CDK's clients.

345. Plaintiffs and Class Members conferred a monetary benefit to Defendant in the form of monies paid for goods or services to Defendant's clients. Upon information and belief, this financial benefit was in, part, conferred when CDK was paid by its clients to provide its DMS services to its clients. CDK also benefitted from the receipt of Plaintiffs' and Class Members' PII. directly and/or indirectly provided Defendant with their PII. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their PII protected with adequate data security.

346. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

347. Defendant enriched itself by saving the costs it reasonably should have expended in data-security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. On the other hand, Plaintiffs and Class Members suffered as a direct and proximate result of Defendant's decision to prioritize its profits over the requisite security.

348. CDK''s unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiffs and Class Members PII, while at the same time failing to securely maintain that information from unauthorized access and compromise.

349. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

350. Defendant failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit of Plaintiffs and Class Members.

351. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

352. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their PII, they would not have agreed to provide their PII to Defendant.

353. Plaintiffs and Class Members have no remedy at law.

354. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer injury, including but not limited to: (i) actual

identity theft, (ii) the loss of opportunity to determine how their PII is used, (iii) the compromise, publication, and/or theft of their PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII, (v) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in its continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

355. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

356. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them and/or their employers. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members and/or their employers overpaid for Defendant's services.

COUNT EIGHT
Declaratory Judgment
(On behalf of the Plaintiffs and the Classes)

357. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

358. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

359. An actual controversy has arisen after the Data Breach regarding Plaintiffs' and Class Members' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continue to suffer injury due to the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

360. Plaintiffs and the Classes have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including: (i) Defendant's failure to encrypt Plaintiffs' and Class Members' PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiffs.

361. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and Class Members;

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII;

c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

362. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law, industry, and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third-party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

363. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

364. The hardship to Plaintiffs, if an injunction is not issued, exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to use such measures.

365. Issuance of the requested injunction will satisfy the public interest. Such an injunction would benefit the public by preventing another data breach at Defendant, thus

eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT NINE
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act
815 ICLS 505/1, et seq.
(On Behalf of Plaintiffs and the Nationwide Class and the Nationwide Consumer/Employee Subclass)

366. Plaintiffs re-allege paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

367. This claim is brought under the Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA").

368. Plaintiffs and Class Members are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e).

369. Plaintiffs, the Classes, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c). 139. The ICFA applies to Defendant because Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

370. Defendant violated ICFA by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and

privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

371. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its omissions.

372. Had Defendant disclosed to Plaintiffs and Class Members (or their third-party agents) that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiffs and Class Members (or their third-party agents) entrusted to it while keeping the inadequate state of its

security controls secret from the public. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

373. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class Members' rights.

374. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

375. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

376. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law. 148. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

377. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, et seq.

378. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the ICFA.

COUNT TEN
Violation of the California Consumer Privacy Act - Cal. Civ. Code § 1798.150(a)
(On behalf of the Plaintiff Baraga and the California Subclasses)

379. Each and every allegation of all previous paragraphs is incorporated in this Count with the same force and effect as though fully set forth herein.

380. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> > (B) Injunctive or declaratory relief.
> > (C) Any other relief the court deems proper.

381. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million and does business in California.

382. Further, Defendant collects and processes Plaintiff Baraga's and California Class Members' personal information within the meaning of the CCPA. When providing its DMS to its clients, CDK was entrusted with, and collected and stored the PII of Plaintiff Baraga and the

California Class. In turn, CDK processes this information to help its clients manage customer relationships, track vehicle sales and vehicle servicing, and otherwise streamline everyday dealership operations.

383. Plaintiff for the California Subclasses and California Class Members are covered "consumers" under § 1798.140(g) in that they are California residents.

384. CDK violated Section 1798.150 of the CCPA by failing to prevent Plaintiff Baraga's and California Class Members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

385. Upon information and belief, Plaintiff Baraga's and California Class Members' PII accessed and compromised by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

386. The personal information of Plaintiff and California Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information CDK collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number; and (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

387. Defendant knew or should have known that its computer systems, its DMS, and data security practices were inadequate to safeguard the Plaintiff's and California Class Members'

personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and California Class Members. Specifically, Defendant subjected Plaintiff's and California Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

388. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and California Class Members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed Defendant's customers' and their employees' personal information.

389. As a direct and proximate result of Defendant's acts, Plaintiff and California Class Members were injured and lost money or property, the loss of Plaintiff's and California Class Members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

390. Cal. Civ. Code Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiff by way of this complaint seeks actual pecuniary damages suffered as a result of CDK's violations described herein. Plaintiff will issue a notice of these alleged violations pursuant to § 1798.150(b) and intends to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

COUNT ELEVEN
Violation of the Florida Deceptive and Unfair Trade Practices Act - Fla. Stat. § 501.201, *et seq.* ("FDUTPA")
(On behalf of the Plaintiff Berman and the Florida Subclass)

391. Plaintiff Berman re-alleges paragraphs 1-277 as if fully incorporated in this Count with the same force and effect as though fully set forth herein.

392. This The FDUTPA, which, pursuant to Fla. Stat. § 501.202, requires such claims be "construed liberally" by the courts "[t]o protect the consuming public and legitimate business enterprises from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce."

393. Defendant's offer, provision, and/or sale of services at issue in this case are "consumer transaction[s]" within the scope of the FDUTPA. *See* Fla. Stat. §§ 501.201-501.213.

394. Plaintiff Berman and the Florida Subclass, as "individual[s]," are "consumer[s]" as defined by the FDUTPA. *See* Fla. Stat. § 501.203(7).

395. Defendant provided services to Plaintiff Berman and the Florida Subclass.

396. Defendant offered, provided, or sold services in Florida and engaged in trade or commerce directly or indirectly affecting the consuming public, within the meaning of the FDUTPA. *See* Fla. Stat. § 501.203.

397. Plaintiff Berman and the Florida Subclass paid for or otherwise availed themselves and received services from Defendant, primarily for personal, family, or household purposes.

398. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the procurement or provision of employment or services to or from Plaintiff Berman and the Florida Subclass.

399. Defendant's acts, practices, and omissions were done in the course of Defendant's businesses of offering, providing, and servicing customers throughout Florida and the United States.

400. The unfair, unconscionable, and unlawful acts and practices of Defendant alleged herein, emanated and arose in party within the State of Florida, within the scope of the FDUTPA.

401. Defendant, conducting extensive business in the State of Florida, engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. failure to implement and maintain reasonable and adequate computer systems and data security practices to safeguard PII;

b. omitting, suppressing, and concealing the material fact that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. failure to protect the privacy and confidentiality of Plaintiff Berman's and the Florida Subclass's PII;

d. continued acceptance and storage of PII after Defendant knew or should have known of the security vulnerabilities that were exploited in the Data Breach; and

e. continued acceptance and storage of PII after Defendant knew or should have known of the Data Breach and before it allegedly remediated the Data Breach.

402. These unfair, unconscionable, and unlawful acts and practices violated duties imposed by laws, including by not limited to the FTC Act, 15 U.S.C. § 41, *et seq.*, and the FDUTPA, Fla. Stat. § 501.171(2).

403. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff Berman's and the Florida Subclass's PII and that the risk of a data breach or theft was high.

404. Plaintiff Berman has standing to pursue this claim because as a direct and proximate result of Defendant's violations of the FDUTPA, Plaintiff Berman and the Florida Subclass have been "aggrieved" by a violation of the FDUTPA and bring this action to obtain a declaratory judgment that Defendant's acts or practices violate the FDUTPA. *See* Fla. Stat. § 501.211(a).

405. Plaintiff Berman also has standing to pursue this claim because, as a direct result of Defendant's knowing violation of the FDUTPA, Plaintiff Berman is at a substantial present and imminent risk of identity theft. Defendant still possesses Plaintiff Berman's and the Florida Subclass's PII, and Plaintiff Berman's PII was exfiltrated by unauthorized third parties, which is evidence of a substantial and imminent risk of future identity theft for all Plaintiff Berman and the Florida Subclass.

406. Plaintiff Berman and the Florida Subclass are entitled to injunctive relief to protect them from the substantial and imminent risk of future identity theft, including, but not limited to:

f. ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems

on a periodic basis, and ordering prompt correction of any problems or issues detected by such third-party security auditors;

g. ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

h. ordering that Defendant audit, test, and train security personnel regarding any new or modified procedures;

i. ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of a network system is compromised, hackers cannot gain access to other portions of the system;

j. ordering that Defendant purge, delete, and destroy PII not necessary for its provisions of services in a reasonably secure manner;

k. ordering that Defendant conduct regular database scans and security checks;

l. ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

m. ordering Defendant to meaningfully educate individuals about the threats they face as a result of the loss of their financial and PII to third parties, as well as the steps victims should take to protect themselves.

407. Plaintiff Berman brings this action on behalf of herself and the Florida Subclass for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow employees and consumers to make informed purchasing decisions and to protect Plaintiff Berman, the Florida Subclass, and the public from

Defendant's unfair methods of competition and unfair, unconscionable, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

408. The above unfair, unconscionable, and unlawful practices and acts by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Berman and the Florida Subclass that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

409. Defendant's actions and inactions in engaging in the unfair unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

410. Plaintiff Berman and the Florida Subclass seek relief under the FDUTPA, Fla. Stat. §§ 501.201, *et seq*., including, but not limited to, a declaratory judgment that Defendant's actions and/or practices violate the FDUTPA.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class and Subclasses, appointing Plaintiffs representatives of the Class and Subclasses, and appointing the undersigned counsel to represent the Class and Subclass;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class ad Subclasses;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class and Subclass;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiffs and the Class and Subclasses damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class and Subclasses in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class and Subclasses leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: April 18, 2025

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com

Andrew J. Shamis (IL Bar No. 6337427)
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Tel: 305-479-2299
ashamis@shamisgentile.com

Interim Co-Lead Counsel for the Putative Class

Gary M. Klinger (IL Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
866.252.0878
gklinger@milberg.com

Interim Liaison Counsel for the Putative Class

Patrick D. Donathen
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(412) 322-9243
patrick@lcllp.com

Maureen Kane Berg (IL Bar No. 6200319)
Lockridge Grindal Nauen PLLP
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
612.339.6900
mkberg@locklaw.com

Jeffrey S. Goldenberg (IL Bar No. 0063771)
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
T: (513) 345-8297
jgoldenberg@gs-legal.com

Interim Co-Lead Counsel for the Putative Employee/Consumer Subclass

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that on April 18, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record, below, via the ECF system.

DATED this 18th day of April, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@straussborrelli.com
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109